UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/607,375	06/30/2000	Curtis E. Ide	05456.105004	8222

7590 07/29/2005

King & Spalding
45th Floor
191 Peachtree Street N E
Atlanta, GA 30303

EXAMINER	
JACKSON, JENISE E	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/607,375	IDE ET AL.	
	Examiner	Art Unit	
	Jenise E. Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *3,4 and 6* is/are allowed.

6)☒ Claim(s) *1,2,5 and 7-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ ~~Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)~~ Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ ~~Notice of Informal Patent Application (PTO-152)~~
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-2, 5, 7-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman(6,510,523) in view of Gleichauf et al(6,324,656).

3. As per claim 1, Perlman et al. discloses authenticating a workstation (i.e. terminal) requesting a network service from a network server via a computer network(see col. 4, lines 39-52), and issues these credentials to perform privileged operations on a remote terminal(see col. 3, lines 62-67, col. 4, lines 1-10, 39-52), generating workstation security credentials based on the (see col. 4, lines 39-40), the workstation security credentials including one of integrity information (see col. 5, lines 1-32), comparing the workstation security credentials to a workstation security policy to determine whether the workstation should be granted access to the network service(see col. 3, lines 62-67, col. 4, lines 1-10), authorizing access to the network service by the workstation if the workstation security credentials satisfy the workstation security policy, otherwise denying access to the network service by the workstation(see col. 6, lines 49-60). Perlman does not disclose completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network; and describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise. However,

Gleichauf et al. discloses completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network; and describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise(see col. 2, lines 6-15, 51-54, col. 3, lines 41-47, col. 4, lines 9-19, 43-55). It would have been obvious to one of ordinary skill in the art at the time of the invention to include a vulnerability assessment of the workstation by Gleichauf with Perlman, because a network vulnerability assessment allows a scanning of the workstation to identify potential vulnerabilities, thus allowing intrusions to be prevented(see col. 2, lines 6-15 of Gleichauf).

4. As per claim 2, Perlman discloses the step of authorizing access to a predetermined level of the network service if the workstation security credentials satisfy a portion of the workstation security policy(col. 3, lines 62-67, col. 4, lines 1-10).

5. As per claim 5, limitations have already been addressed(see claim 1). Perlman et al. discloses wherein the step of generating the workstation security credentials(see col. 4, lines 39-65).

6. As per claim 7, limitations have already been addressed see claim 1. Further, as per claim 7, Perlman discloses the assessment server operating as a remote server different from the network server, the network workstation assessment service operative to generate the workstation security credentials (col. 4, lines 39-52).

7. As per claim 8, limitations have already been addressed(see claim 1).

8. As per claim 9, Perlman et al. discloses the step of communicating a service decision from the network server to the workstation via the computer network, the service decision

defining whether the workstation is allowed to access the network service(see col. 3, lines 62-67, col. 4, lines 1-10, col. 6, lines 43-48).

9. As per claim 10, limitations have already been addressed see claim 1. Also as per claim 10, Perlman et al. discloses wherein the step of generating the workstation security credentials (col. 3, lines 62-67, col. 4, lines 1-10).

10. As per claim 11, Perlman et al. discloses wherein the workstation security policy is maintained on the network server, the process further including the step of comparing at the network server the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the network service(see col. 4, lines 1-10, 39-52).

11. As per claim 12, it is rejected under the same basis as claim 1.

12. As per claim 13, limitations have already been addressed(see claim 1).

13. As per claim 14, Perlman et al. discloses including a workstation security policy at the network server, the workstation security policy operative to define security requirements for secure operation of the workstation on the computer network(see col. 3, lines 62-67, col. 4, lines 1-10)

14. As per claim 15, Perlman et al. discloses wherein the network service is further operative for comparing the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the software service (col. 6, lines 3-17), the network service operative to authorize access to the software service by the workstation if the workstation security credentials satisfy the workstation security policy (see col. 6, lines 49-60).

15. As per claim 16, limitations have already been addressed(see claim 1).

16. As per claims 17, 22, limitations have already been addressed(see claim 14).

17. As per claims 18, 23, limitations have already been addressed(see claim 15).

18. As per claim 19, limitations have already been addressed(see claim 1). Also, as per claim 19, Perlman et al. discloses issuing a request for a log-in page to a network server from a browser operating on the workstation(see col. 3, lines 50-57); transmitting the log-in page and an authentication plug-in from the network server to the workstation via the compute network, the authentication plug-in installable within the browser(see col. 3, lines 5-57, col. 4, lines 53-65) and operative to generate workstation security credentials by completing a (see col. 3, lines 62-67, col. 4, lines 1-10, 39-52); transmitting the workstation security credentials from the authentication plug-in to the network server via the computer network; and determining at a CGI script operating on the network server whether the workstation should be granted access to a software service of the network based on the workstation security credentials(see col. 3, lines 50-60, col. 4, lines 39-52).

19. As per claim 20, limitations have already been addressed(see claim 1). Further, claim 20, Perlman inherently discloses CGI script, because Perlman discloses the Internet (see col. 3, line s50-57, col. 4, lines 63-65)

20. As per claim 21, limitations have already been addressed(see claim 1).

21. As per claim 24, Perlman et al. discloses wherein the network service is operative to transmit to the network assessment service via the computer network a request to complete the vulnerability assessment of the workstation in response to receiving a request for the software service from the workstation (see col. 3, lines 62-67, col. 4, lines 1-10, 39-52).

22. As per claim 25, limitations have already been addressed(see claim 19).

23. Claims 3-4, and 6 are allowable. The reason why these claims are allowable, is for the local assessment service to be maintained on the workstation, the local assessment service(i.e. vulnerability scanner), scans the workstation for vulnerabilities before the credentials are generated. The scanning of the prior art, is done at the server **a network scanner for security checking of application programs (e.g. Java applets or Active X controls) received over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. Static scanning at the HTTP proxy server identifies suspicious instructions and instruments them e.g. a pre-and-post filter instruction sequence or otherwise.** This is an example of prior art that does not disclose the local assessment service being done of the workstation, further, there is no mention of generating credentials after the assessment has been scanned(6, 272, 641). The scanning is done first, to determine if the workstation is malicious or untrusted, and then specific credentials are given. The workstation in security, that is identified is malicious is done by the server, in security.

Response to Amendment

24. The Applicant argues that Perlman does not disclose a vulnerability assessment scan that fins evidence of a compromise. The Examiner has relied upon another reference for the limitations of a vulnerability assessment therefore, the argument is moot.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

July 21, 2005

7/25/05